Avoiding Cyber-Risk Lemons In Due Diligence

By Vince Dasta

Vince Dasta is director of engagements at VisibleRisk.

Mergers and acquisitions (M&A) have traditionally been tools to accelerate growth, optimize costs, and streamline operations. But what happens when the acquiring company ends up buying a cybersecurity incident?

Economist George A. Akerlof's seminal 1970 paper, "The Market for Lemons: Quality Uncertainty and the Market Mechanism," asserts that because a buyer does not know the quality of a product being offered by a seller before buying it, they risk buying a lemon. Like the clichéd used-car example, the same principle applies to much larger and more complex transactions such as M&A.

M&A transactions usually involve CEOs, chief financial officers, accountants, lawyers, and auditors. What these teams often lack is the required cybersecurity expertise to uncover potential "cyber-risk lemons."

THE REAL VALUE OF INFORMATION

In 2016, Marriott International acquired Starwood Hotels and Resorts Worldwide for $13.6 billion. Unbeknownst to both, Starwood's reservation system had been breached in 2014, exposing the personal data of hundreds of millions of customers. Because the breach wasn't detected until after the acquisition, Marriott was fined $24 million for General Data Protection Regulation violations and faces the prospect of hundreds of millions of dollars in legal and compliance costs stemming from a combined 11 class action lawsuits. In 2017, Yahoo! and Verizon Communications agreed to cut $350 million from the price that Verizon would pay for Yahoo's Internet business due to unknown costs related to two large data breaches that were not disclosed until after the deal was agreed to and announced. The two companies also agreed to share liabilities related to the breaches.

A common complaint is that cybersecurity is too complex to evaluate quickly given the lack of a "cyber balance sheet" to review and audit. But reducing cyber-risk uncertainty in an acquisition target isn't as hard as you might think. The timeliness of diligence information is also important: information value is perishable, and an acquisition opportunity may evaporate before a detailed cybersecurity assessment can be completed.

WHAT CAN THE BOARD DO?

An acquirer can investigate past disclosures and ask for the details of any incident investigations and compliance-related findings. But these findings will only provide information about known issues and rely on past self-assessments and audits. Another approach is to conduct an "outside-in" assessment where a target company's public-facing infrastructure and technology footprint are examined. It is better to combine this with an "inside-out" assessment of the target, where critically important compliance requirements and controls are examined and interviews are conducted with key personnel to understand cybersecurity culture and processes.

The time between the public announcement of an M&A transaction and its closing is an especially vulnerable one because sensitive documents are being exchanged, which increases the likelihood of accidental disclosure. For this reason, limiting the number of third parties involved in any cybersecurity evaluation can reduce the likelihood of an incident occurring during the acquisition process.

While it is impossible to completely eliminate uncertainty around the cyber risks being acquired along with a business, leveraging a holistic, business-focused, and independent assessment methodology can greatly reduce the probability of buying a cyber-risk lemon.